IN THE CLAIMS:

Please amend the following claims:

Please cancel claims 1-11, 13, 17-22, and 24-35 without prejudice.

1-11. (Canceled)

12. (Currently Amended) ~~The system of claim 10~~ A system for securely processing transactions, the system comprising:

a security key device, comprising,

a user authenticator configured to provide a user an authentication data input for proving the user is authorized to use an account associated with the security device,

a first counter in communication with the user authenticator,

a key generator in communication with the user authenticator and first counter, the key generator being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from contents of the first counter, and

an electronic display in electrical communication with the key generator, for displaying the security key in a manner visible upon the structure; and

an authorization device, comprising,

a second counter, and

a key confirmation processor programmed to confirm an authenticity of the security key in a manner at least partially dependent upon the contents of the second counter,

wherein the security key is derived at least partially from the contents of the first counter,

wherein the key confirmation processor approves a transaction if the contents of the first counter matches contents of the second counter within a predetermined range.

13. (Canceled)

14. (Currently Amended) ~~The system according to claim 9~~ A system for securely processing transactions, the system comprising:

a security key device, comprising,

a user authenticator configured to provide a user an authentication data input for proving the user is authorized to use an account associated with the security device,

a first counter in communication with the user authenticator,

a key generator in communication with the user authenticator and first counter, the key generator being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from contents of the first counter, and

an electronic display in electrical communication with the key generator, for displaying the security key in a manner visible upon the structure; and

an authorization device, comprising,

a second counter, and

a key confirmation processor programmed to confirm an authenticity of the security key in a manner at least partially dependent upon the contents of the second counter, wherein:

the security key device further comprises a first clocking mechanism having an output coupled to the key generator, and the key generator programming includes use of the clocking mechanism output to generate the security key;

the authorization device further comprises a second clocking mechanism synchronized to the first clocking mechanism, and a second counter; and

the key confirmation processor is programmed to confirm an authenticity of the key in a manner at least partially dependent upon the contents of the second counter and an output of the second clocking mechanism.

15. (Currently Amended) The ~~device~~ system according to claim 14, wherein the clocking mechanisms are based on a time variant device.

16. (Currently Amended) The ~~device~~ system according to claim 14, wherein said clocking mechanisms are based on actual time.

17-22. (Canceled)

23. (Currently Amended) ~~The method according to claim 21~~ A method of securely authorizing a transaction utilizing an account, the method comprising:

confirming an authorized use of an account card via a PIN provided by a user;

maintaining a first count indicative of a number of instances of such authorized uses;

generating a security key in a manner at least partially dependent upon the count;

transmitting the security key to an authorizing authority;

processing the security key at the authorizing authority;

maintaining a second count indicative of a number of transmissions received by the authorizing authority for the account;

confirming that the security key was generated by an authorized user at least in part through use of the second count;

authorizing the transaction if the security key was generated by an authorized user,

wherein the security key is generated using an encryption algorithm to process a card key and the first count,

wherein the transaction is authorized if the first count is within a predefined number of the second count,

further comprising the step of:

maintaining first and second clocking devices configured to respectively produce first and second clock signals;

wherein:

said step of generating a security key comprises generating a security key in a manner at least partially dependent upon the count and the first clocking device; and

said step of confirming the security key comprises confirming that the security key was generated by an authorized user at least in part through use of the second count and the second clock signal.

24-35. (Canceled)

36. (Original) A smart card, comprising,

an activation device configured to produce a signal in response to a user action;

a display mechanism;

a processing device coupled to the display device and configured to receive said signal; and

programming executable by the processing device upon receipt of said signal and configured to produce an encrypted key and display the encrypted key on the display mechanism;

wherein:

said smart card comprises a credit card sized enclosure;

said display mechanism is disposed on a face of the credit card sized enclosure;

said programming is stored on a computer readable media disposed on or within the credit card sized enclosure;

said credit card sized enclosure in a solid flexible material;

said activation device is a numeric entry system disposed on a face of the credit card sized enclosure;

said numeric entry system includes a ten key type entry system and said user action is entry of a PIN via the numeric entry system;

said programming is further configured to verify said user action prior to displaying the encrypted key;

if said programming is unable to verify said user action, then, displaying one of an error message and a non-authentic value on the display mechanism;

said smart card further comprises a bio-metric sensing device coupled to said processing device;

said programming is further configured to retrieve a bio-metric input from said bio-metric sensing device and compare the bio-metric input to a stored bio-metric value prior to one of calculating and displaying the encrypted key,

said bio-metric sensing device is a fingerprint scanner;

said smart card further comprises a transaction counter configured to track authorized transactions associated with the smart card and a clocking mechanism configured to produce a time varying clock value;

said encrypted key is derived, at least in part, based on the transaction counter and time varying clock value; and

said smart card is capable of communicating with an authorization device that,

retrieves the encrypted key from a PIN field of a transaction communication,

decrypts the encrypted key using a count from a second transaction counter and a second time varying clock value from a second clocking mechanism synchronized with the first clocking mechanism, and

authorizes a transaction if the decrypted key is valid;

the decrypted key being valid if produced by the smart card with a valid PIN and the first and second transaction counters are synchronized within a predetermined number of transactions.